AO 93 (Rev. 12/09) Search and Seizure Warrant (USAO CDCA Rev. 01/2013)

ORIGINAL

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

26572 Paseo Callado
San Juan Capistrano, California

Case No. SA 15-588M

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A-1

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

FILED
2016 AUG 10 PM 1:42
CLERK U.S. DISTRICT COURT
C.D. DIST. OF CALIF.
SANTA ANA

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/8/2016 2:08 pm

Judge's signature

City and state: Santa Ana, CA

HON. ~~JAY C. GANDHI~~

Printed name and title

Jay C. Gandhi

AUSA: J. Waier

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
15-588M	12/8/15 17:00	Trent Westcott (owner)

Inventory made in the presence of: HSI SA Mark Hanson (evidence custodian)

Inventory of the property taken and name of any person(s) seized:

[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

search warrant executed without incident on 12/8/15 at 17:00. See attached inventory of items seized. Both digital devices returned on 2/3/16.

HSI case #: OR08NE100R0009

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: 8/10/16

Executing officer's signature

Brent Regan / Special Agent

Printed name and title

AUSA: J.Waier

DEPARTMENT OF HOMELAND SECURITY

No. 6450403

CUSTODY RECEIPT for SEIZED PROPERTY and EVIDENCE

Handbook 5200-09

1. FPF No.	2. Incident No.
3. Investigative Case No. 0R08NE100R0009	4. Enforce No.
5. Prior Detention? Yes ☐ No ☐ If yes, DHS 6051D No._____	6. Date Seized (mm/dd/yyyy) 12/03/2015 / 7. Time Seized (Use 24 Hrs) / 8. FDIN/Misc.
9. Seized From: Name: Westcott Address: 26572 Paseo Collado San Juan Capistrano, CA Telephone No. ( ) Ext:	10. Entry No. / 11. Seal or Other ID Nos. 12. Remarks:

13. Send Correspondence to:

14. **PROPERTY** (By Line Item) Attach DHS Form 58 if conveyance

a. Line Item No.	b. Description	c. Packages Number	c. Packages Type	d. Measurements Qty.	d. Measurements UM	e. Est. Dom. Value
001	Samsung Galaxy S6	1	CA			$
002	Asus Laptop Model TP500L F3NOWU0945951G	1	CA			$
						$
						$
						$
						$

15. Seizing Officer: Mark Hanson (Print Name) x [signature] (Signature) 12/8/15 (Date)

16. **ACCEPTANCE / CHAIN OF CUSTODY**

a. Line Item No.	b. Description	c. Print Name/Title/Organization	d. Signature	e. Date
1-2	AS NOTED ABOVE	Whitaker/SA/HSI	[signature]	12/8/15
1&2	"	Ryan Lee/SA/HSI	[signature]	1/4/16
1&2	"	TFO/M Wescott	[signature]	2/3/16

DHS Form 6051A Continuation Sheet Attached? Yes ☐ No ☐

DHS retains original
Previous editions are obsolete

DHS Form 6051S (08/09)

DEPARTMENT OF HOMELAND SECURITY

No. 6450404

CUSTODY RECEIPT for SEIZED PROPERTY and EVIDENCE

Handbook 5200-09

1. FPF No. 270160500035001	2. Incident No. 2016520020174001
3. Investigative Case No. OPOSNE100PC0007	4. Enforce No.
5. Prior Detention? Yes ☐ No ☐ If yes, DHS 6051D No.	6. Date Seized (mm/dd/yyyy) 12/9/2015 / 7. Time Seized (Use 24 Hrs) 1945 0200 / 8. FDIN/Misc.
9. Seized From: Name: Westcott Address: 26572 Paseo Callado San Juan Capistrano, CA Telephone No. ( ) Ext:	10. Entry No. / 11. Seal or Other ID Nos. 12. Remarks:
13. Send Correspondence to:	

14. **PROPERTY** (By Line Item) Attach DHS Form 58 if conveyance

a. Line Item No.	b. Description	c. Packages Number	c. Packages Type	d. Measurements Qty.	d. Measurements UM	e. Est. Dom. Value
003	Financial Papers	1	bx	4	ea	$
						$
						$
						$
						$
						$

15. Seizing Officer

Print Name		Signature	Date
Mark Hanson	x		12/8/15

16. **ACCEPTANCE / CHAIN OF CUSTODY**

a. Line Item No.	b. Description	c. Print Name/Title/Organization	d. Signature	e. Date
003	FINANCIAL PAPERS	P. DIAZ SA/HSI		5/20/16

DHS Form 6051A Continuation Sheet Attached? Yes ☐ No ☐

DHS retains original
Previous editions are obsolete

DHS Form 6051S (08/09)

AFFIDAVIT

I, Special Agent Brent Rogan, being duly sworn, do hereby depose and state the following:

BACKGROUND OF AFFIANT

1. I am a Special Agent of the Department of Homeland Security, United States Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), assigned to the Office of the Assistant Special Agent in Charge, Orange County. I have been a Special Agent with HSI for over eight years. As part of my duties, I currently investigate violations of criminal law relating to the illegal importation of contraband, including counterfeit goods and controlled substances, intellectual property rights violations and related money laundering. My duties consist of enforcing the Tariff Act and other laws, rules and regulations governing the import and export of goods and merchandise and payment of duties and fees.

2. During my career, I have conducted and participated in numerous complex, multi-defendant investigations involving commercial fraud, money laundering, manufacture of fraudulent documents, marriage fraud, drug trafficking and related financial crimes. I have conducted and participated in investigations that have

resulted in the identification, seizure and federal forfeiture of millions of dollars in cash and assets and the seizure and forfeiture of millions of dollars in counterfeit goods. I have also been responsible for the detection, arrest and conviction of numerous individuals.

3. As part of my employment, I have received training from ICE and Customs and Border Protection ("CBP") related to investigative techniques and the conduct of fraud, IPR and financial investigations. I have a working knowledge relating to commercial fraud, including under-valuation, misclassification and trademark/copyright violations.

PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of an application to search: (1) the premises of 26572 Paseo Callado, San Juan Capistrano, California (the "RESIDENCE PREMISES"), a residence owned by Michael Westcott ("WESTCOTT"), which is further described in Attachment A-1 and (2) Lightning Technology Inc. ("LIGHTNING"), 970 Calle Negocio, San Clemente, California 92673 (the "BUSINESS PREMISES"), a business owned and by Westcott, which is further described in Attachment A-2 (collectively the "SUBJECT PREMISES").

5. As set forth below, there is probable cause to believe that located at the SUBJECT PREMISES is evidence of a conspiracy to distribute, traffic, and sell counterfeit copies of copyrighted or trademarked Cisco Systems Inc. ("CISCO") products, in violation of Title 17, United Stated Code, Section 506 - Criminal Infringement, Title 18, United States Code, Section 371 - Conspiracy, Section 1341 - Mail Fraud, Section 1343 - Wire Fraud, Section 2318 - Trafficking in counterfeit labels, Section 2319 - Criminal Infringement of a Copyright, and Section 2320 - Trafficking in Counterfeit Goods or Services, and is fully described in Attachment B.

6. The facts set forth in this affidavit are based my own observations, upon my personal review of the documents described herein, information obtained from other Special Agents and witnesses, and my own training and experience. This affidavit is intended to show that there is sufficient probable cause for the requested search warrant and does not purport to set forth all of my knowledge of, or all the knowledge of other ICE Special Agents, or of the investigation into this matter. In addition, when relying on statements made by others, such statements are set forth in substance and in pertinent part, not verbatim.

OVERVIEW OF THE COUNTERFEIT CISCO SCHEME

7. In 2010, HSI became aware, through customs seizures described below, that LIGHTNING located at the BUSINESS PREMISES was importing counterfeit Cisco labels and blank computer hardware and selling then as genuine Cisco product.

8. Based on the seizures of international shipments of LIGHTNING, undercover buys, and surveillance (described below), LIGHTNING has sold to end users, or tried to smuggle, into the United States counterfeit Cisco products/labels worth over one million dollars.

WESTCOTT OWNS AND OPERATES LIGHTNING AT THE BUSINESS PREMISES AND RESIDES AT THE RESIDENCE PREMISES

9. On December 7, 2015, I reviewed the LIGHTNING web site and OC-IT web site and learned the following:

a. WESTCOTT is the President and founding partner of LIGHTNING, which he has been operating since 1995.

b. LIGHTNING is located at the BUSINESS PREMISES.

c. LIGHTNING is a "source" to buy or lease computer networking, Telecom, and Storage equipment, including. The LIGHTNING web site has a contact page that allows the customer to put in their information and receive a quote on computer parts from LIGHTNING.

d. WESTCOTT is also President and Chief Executive Officer of OC-IT.com, which is also located in the BUSINESS PREMISES. OC-IT.com provides network security and administration services, including support for Cisco products. WESTCOTT listed OC-IT as his employment on the rental application where the counterfeit Cisco labels were picked up by WESTCOTT on December 7, 2015 as described in paragraphs 17f and 17g below.

e. LIGHTNING uses computers to run its business. Both undercover buys described below were done using the internet. In the undercover buy I conducted, I received a quote for the computer parts from LIGHTNING through email. When I received the computer parts from LIGHTNING, there was a printed invoice that appeared to be generated by a computer.

f. Based on my training and experience, businesses keep track of inventory, imports, customers, and sales on computers.

10. On December 2, 2015, December 3, 2015, and December 7, 2015, I and other agents conducted surveillance at the BUSINESS PREMISES and saw WESCOTT at the BUSINESS PREMISES during business hours.

11. According to the California Department of Motor Vehicles, WESTCOTT lists the RESIDENCE PREMISES on his California Driver's License.

12. On December 2, 2015, I and other agents were surveilling both the RESIDENCE and BUSINESS PREMISES and observed WESCOTT leave from the BUSINESS PREMISES at approximately 5:10 p.m. and arrive at the RESIDENCE PREMISES at approximately 5:25 p.m.

13. On December 3, 2015, I and other agents conducted surveillance at both the RESIDENCE and BUSINESS PREMISES and observed WESCOTT leave from the RESIDENCE PREMISES at approximately 7:05 p.m. and arrive at the BUSINESS PREMISES at approximately 7:25 p.m.

14. On December 3, 2015, HSI agents did a trash pull at the RESIDENCE PREMISES. In the trash, HSI agents found documents related to LIGHTNING.

15. On December 7, 2015, I and other agents were surveilling both the RESIDENCE and BUSINESS PREMISES and observed WESCOTT leave from the BUSINESS PREMISES at approximately 4:30 p.m. and arrive at the RESIDENCE PREMISES at approximately 5:04 p.m. HSI agents saw WESTCOTT leave the BUSIENSS PREMISES with documents and take them to the RESIDENCE PREMISES.

WESTCOTT AND LIGHTNING ARE NOT AUTHORIZED TO SELL CISCO PRODUCTS

16. On December 7, 2015, I received an e-mail from a Cisco representative, Tim Casto ("Casto"), a brand protection investigator employed by Cisco. Castro stated that Cisco conducted a query of their database and determined that neither WESTCOTT nor LIGHTNING were "Cisco Authorized Resellers," which means that neither WESTCOTT nor LIGHTNING had signed Cisco's International Channels Partner Agreement (ICPA), which is a contract that would allow a company to purchase Cisco products through Cisco Distributors or in some cases, directly from Cisco.

SEIZED SHIPMENTS OF LIGHTNING AND WESTCOTT CONFIRM THE COUNTERFEIT CISCO SCHEME

17. Based on a review of Customs and Border Protection ("CBP") documents, I learned the following:

a. Between August 30 and August 31, 2007, CBP seized three shipments of counterfeit Cisco products worth a combined $469,925 that were intended for delivery to LIGHTNING at a prior business address on Calle Perfecto in San Juan Capistrano. Based on CBP shipment records, LIGHTNING moved the business to the BUSINESS PREMISES in or about July 2009. All three shipments were sent to LIGHTNING from a company listed as CHAO SHI KONG CO. LTD in

Shenzhen, China. Based on my training and experience, CHAO SHI LONG CO. manufactures counterfeit CISCO products. All three shipments contained transceivers that were affixed with counterfeit Cisco labels.

b. On April 13, 2010, CBP seized a shipment of counterfeit Cisco labels intended for delivery to "Michael" at a post office box located in San Juan Capistrano. LIGHTNING was listed as the consignee. On April 14, 2010, HSI agents attempted a controlled delivery of the counterfeit Cisco labels to WESCOTT at the UPS store in San Juan Capistrano, but were unable to observe WESTCOTT attempting to retrieve the parcel. During this time, HSI agents conducted several trash pulls at the BUSINESS PRESMISES and found counterfeit CISCO labels in the trash. In the package were 224 counterfeit Cisco labels with an infringement value of $248,190. Based on a report of this incident that I reviewed, I learned that later in April 2010, the manager of the UPS store called HSI and reported that WESTCOTT had tried to pick up the package of counterfeit Cisco labels.

c. On August 11, 2012, CBP seized a shipment of four counterfeit Cisco transceivers worth approximately $56,000 that were intended for delivery to "Sepi Westcott," WESTCOTT's wife at the RESIDENCE PREMISES.

d. On July 2, 2013, CBP detained a parcel being delivered to "Mr. Michael" at post office box at a UPS store in Laguna Niguel that contained optical receivers. The items bore no trademarks, but each piece was labeled with an easily removable sticker bearing a part number or serial number. Since no trademark violation was apparent, the parcel was released. Based on my training and experience, these are consistent with blank computer parts that could be labeled with counterfeit Cisco labels. HSI agents viewed the surveillance video from the Laguna Niguel UPS store and saw WESTCOTT picking up the package on July 3, 2013.

e. On August 28, 2015, CBP seized a shipment of 166 counterfeit Cisco transceivers worth approximately $85,250 that were intended for delivery to a UNOCAL 76 gas station located approximately six miles from the LIGHTNING business address. Through an examination of customs records, I learned that this UNOCAL 76 station has been linked to WESTCOTT and LIGHTNING on over 100 previous imports of networking equipment like transceivers. Additionally, according to business registration records maintained by the office of the California Secretary of State, Corporations Division, Michael Nejad is listed as the Corporation Officer and Registered Agent. On

December 7, 2015, I queried the Consolidated Lead Evaluation and Reporting (CLEAR), a commercially available database of public records, and observed that Michael Nejad appears to be related to Sepideh Nejad Westcott, WESTCOTT's wife.

f. On December 2, 2015, CBP seized a package to "MIKE" for delivery at a Mail Boxes Irvine store located at 4521 Campus Drive #278, Irvine, California. I went to the store and reviewed the opening documents for box #278, which shows that WESTCOTT rented #278. The package contained 183 counterfeit Cisco labels that were worth approximately $502,085. Attached as Exhibit A is a picture of the labels.

g. I photographed the contents of the package and allowed the labels to be delivered to the store. I reviewed surveillance footage from the store and saw that on December 7, 2015, Westcott picked up the package of counterfeit Cisco label at 2:30 p.m. At 3:27 p.m. on December 7, 2015, WESTCOTT was seen at the BUSINESS PREMISES.

h. In total, CBP has made 8 seizures of hardware (from 2006 to 2015) that are valued at $952,250 and 3 seizures of labels (the associated products would be valued

at $889,275 from 2009 to 2015) that were intended for delivery to LIGHTNING or WESTCOTT.

UNDERCOVER PURCHASES CONFIRM THE COUNTERFEIT CISCO SCHEME

18. Based on information from Cisco and my own investigation, I learned the following:

a. On November 10, 2013, Cisco investigators conducted a test buy from the LIGHTNING storefront ("ltiauctions") on eBay for one new original Cisco GLC-SX-MM transceiver listed on the LIGHTNING eBay storefront as "Cisco: GLC-SX-MM-NEW: Cisco 1000 Base SX Multimode GBIC NEW." Cisco and Finisar, the Original Equipment Manufacturer ("OEM") for this product, tested the transceiver and confirmed that the transceiver purchased from LIGHTNING was counterfeit. The transceiver was shipped from the BUSINESS PREMISES.

b. On October 16, 2014, I conducted an undercover purchase of three Cisco transceivers (GLC-SX-MM) from LIGHTNING. LIGHTNING shipped the three Cisco transceivers to me from the BUSINESS PREMISES. Cisco and Finisar tested the receivers and determined they were counterfeit.

ADDITIONAL INFORMATION

19. While there have been numerous seizures of counterfeit Cisco products related to the this investigation, LIGHTNING does, in fact, import, distribute and/or sell some legitimate Cisco products.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES

20. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on

a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting

a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the

data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of

peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

21. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

CONCLUSION

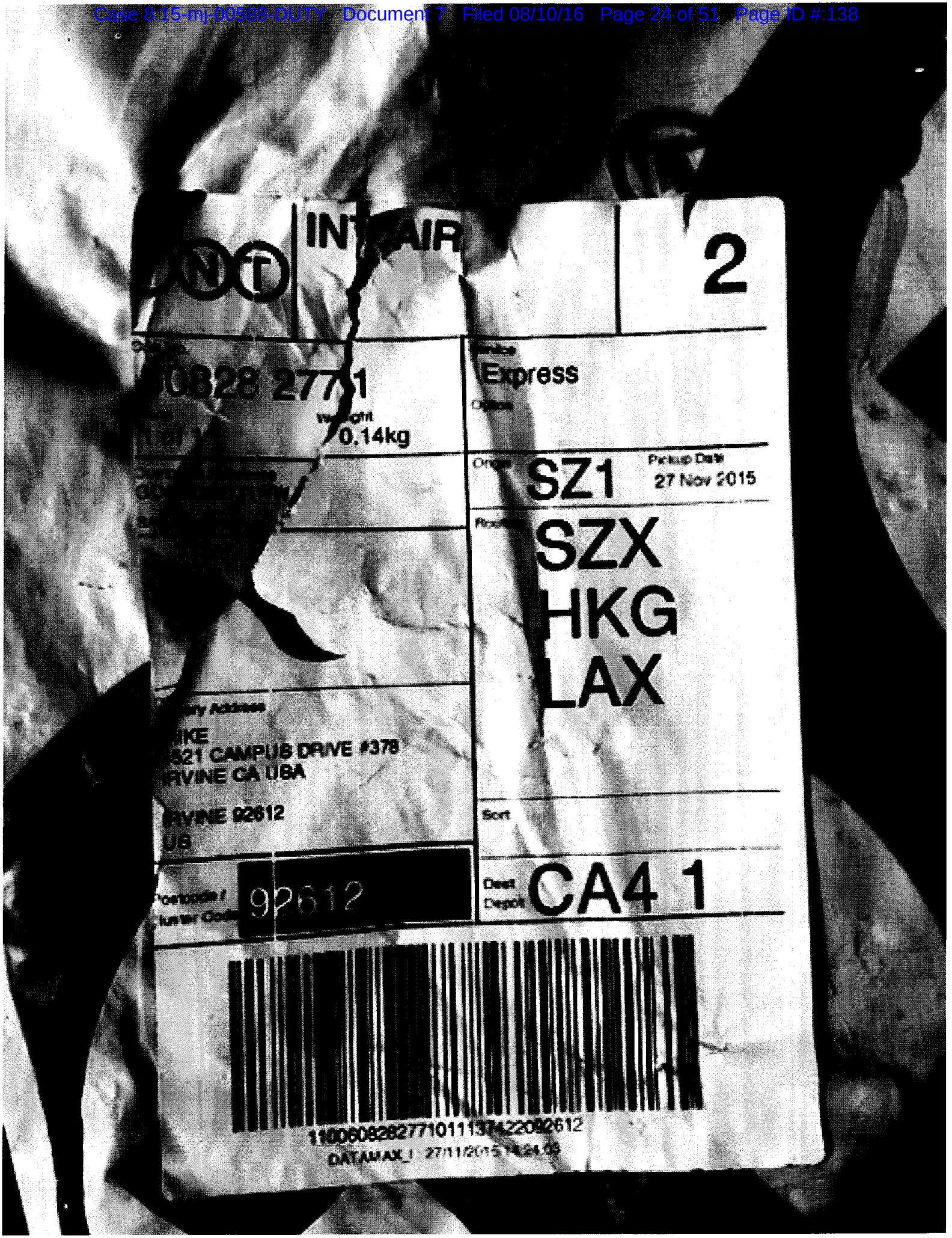
22. Based on the facts set forth herein, I submit there is probable cause to believe that evidence of violations of Title 17, United Stated Code, Section 506 - Criminal Infringement, Title 18, United States Code, Section 371 - Conspiracy, Section 1341 - Mail Fraud, Section 1343 - Wire Fraud, Section 2318 - Trafficking in counterfeit labels, Section 2319 - Criminal Infringement of a Copyright, and Section 2320 - Trafficking in Counterfeit Goods or Services will be discovered at the SUBJECT PREMISES.

BRENT ROGAN
Special Agent, HSI

Subscribed and sworn to before me
this 11th day of December 2015.

United States Magistrate Judge
Jay C. Gandhi

EXHIBIT A


NOT
IN AIR
2
0828 2771
0.14kg
Express
SZ1
Pickup Date
27 Nov 2015
SZX
HKG
LAX
IKE
521 CAMPUS DRIVE #378
RVINE CA USA
RVINE 92612
US
92612
CA4 1
DATAMAX_I

ATTACHMENT A-1

PREMISES TO BE SEARCHED

The RESIDENCE PREMISES is located at 26572 Paseo Callado, San Juan Capistrano, CA 92675 and further described as:

The structure is located at 26572 Paseo Callado on the south side of Paseo Callado in the city of San Juan Capistrano, California. It is a beige single family residence with a red brick façade on the front of the residence, a brown Spanish tile roof, red-brown shutters around the windows and a red-brown front door that matches the shutters. According to real estate websites, the residence is described as a 5 bedroom, 4 1/2 bath, single family home, approximately 3,593 total square feet in size. The residence is a two story structure, built on top of an elevated lot, with an attached 2-car garage with a brown roll-up door and 12 tinted windows. A glass door on the second story of the front of the residence opens to a small balcony directly above the front door. The house number "26572" appears in black letters on a white oval-shaped sign located on the stucco on wall to the left side of the garage door. Satellite images available on www.google.com/maps show what appears to be a patio, landscaped backyard, and swimming pool to the rear of the residence.

The RESIDENCE PREMISES includes any attached or unattached structures, garages, attics, basements, and assigned trash receptacles.

ATTACHMENT A-2

PREMISES TO BE SEARCHED

The BUSINESS PREMISES is LIGTNING TECHNOLOGY, INC. located at 970 Calle Negocio, San Clemente, CA 92673 and further described as:

The BUSINESS PREMISES is a commercial office building located at 970 Calle Negocio, San Clemente, CA 92673. The sides of the building appear to be a stone facade, tan in color, with a pattern of large squares, approximately six feet in size cut into the facade. A white stripe appears at or near the top of the exterior walls of the building. The building number "970" appears in large numbers attached to the southeast side of the structure near the top above the white stripe. The "9" appears white in color and the "70" portion of the number appear black. Below and to the right of the building number is a business sign that reads "OC-IT.com" that includes a logo of three dots connected by two lines. Around the corner to the left of the building number, as viewed from the front of the building, the "OC-IT.com" sign and logo appear again. On both signs, the "OC" letters appear orange, the "IT" letters appear blue, and the "-" and the ".com" appear black. To the left the two "OC-IT.com" signs, as viewed from the front of the building, a third sign appears below the white stripe at the top of the wall that reads "Lightning Technology." The word "Lightning" in the sign

appears in green letters with the exception of the first "i" which appears as a large red lightning bolt. The word "Technology" appears below in black letters.

The public entrance to the BUSINESS PREMISES is located under the above-described signs on the southwest corner of the building. The door appears to be tinted glass in a white metal frame and the wall surrounding this door also appears to be tinted glass of the same shade with white metal trim arranged in a pattern of squares approximately three feet in size.

The BUSINESS PREMISES also has a pedestrian door on the rear of the structure on the northwest corner and a roll-up style warehouse door to the north of the pedestrian door.

The business entities "OC-IT.com" and "Lightning Technology" appear to share the same office space at 970 Calle Negocio, but the business space appears to be distinct from the attached space at 972 Calle Negocio which is described by a sign on the building at "San Clemente Gymnastics."

The BUSINESS PREMISES includes any attached or unattached structures, warehouses, garages, attics, basements, and assigned trash receptacles.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 17, United Stated Code, Section 506 - Criminal Infringement, Title 18, United States Code, Section 371 - Conspiracy, Section 1341 - Mail Fraud, Section 1343 - Wire Fraud, Section 2318 - Trafficking in Counterfeit Labels, Section 2319 - Criminal Infringement of a Copyright, and Section 2320 - Trafficking in Counterfeit Goods from March 2008 to the present, specifically:

a. Counterfeit Cisco transceivers, routers, switches, and computer networking equipment, and any accompanying accessories, labels, marks, letters of authenticity, and packaging.

b. Any document referencing or referring to counterfeit Cisco products or labels.

c. Any items bearing registered trademarks of Cisco.

d. Records, documents, programs, applications, and materials reflecting or referencing the importation, exportation, purchase, possession, transfer, distribution, or sale of Cisco transceivers, routers, switches, computer networking equipment, labels, and/or packaging.

e. Records, documents, programs, applications, and materials filed with U.S. Customs and Border Protection in

connection with the importation, exportation, purchase, possession, transfer, distribution, or sale of Cisco transceivers, routers, switches, computer networking equipment, labels, and/or packaging.

f. Business bank account records, wire transfer records, bank statements and records, money drafts, letters of credit, and financial transfers that reflect the money generated from the importation, exportation, purchase, possession, transfer, distribution, or sale of Cisco transceivers, routers, switches, and computer networking equipment.

g. Limited to 15 items per SUBJECT PREMISES, any records, documents, programs, applications, and materials that show indicia of occupancy, residency, control and/or ownership of the SUBJECT PREMISES, including but not limited to, utility bills, telephone bills, loan payment receipts, rent documents, canceled envelopes and keys, photographs, and bank records.

h. Records, documents, programs, applications, and materials reflecting off-site storage facilities owned, used, or operated by LIGHTNING TECHNOLOGY INC., OC-IT.COM, or MICHAEL WESTCOTT.

i. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

j. With respect to any digital device used to facilitate the above-listed violations or containing evidence

falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical

disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of

items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT A-1

PREMISES TO BE SEARCHED

The RESIDENCE PREMISES is located at 26572 Paseo Callado, San Juan Capistrano, CA 92675 and further described as:

The structure is located at 26572 Paseo Callado on the south side of Paseo Callado in the city of San Juan Capistrano, California. It is a beige single family residence with a red brick façade on the front of the residence, a brown Spanish tile roof, red-brown shutters around the windows and a red-brown front door that matches the shutters. According to real estate websites, the residence is described as a 5 bedroom, 4 1/2 bath, single family home, approximately 3,593 total square feet in size. The residence is a two story structure, built on top of an elevated lot, with an attached 2-car garage with a brown roll-up door and 12 tinted windows. A glass door on the second story of the front of the residence opens to a small balcony directly above the front door. The house number "26572" appears in black letters on a white oval-shaped sign located on the stucco on wall to the left side of the garage door. Satellite images available on www.google.com/maps show what appears to be a patio, landscaped backyard, and swimming pool to the rear of the residence.

The RESIDENCE PREMISES includes any attached or unattached structures, garages, attics, basements, and assigned trash receptacles.

ATTACHMENT A-2

PREMISES TO BE SEARCHED

The BUSINESS PREMISES is LIGTNING TECHNOLOGY, INC. located at 970 Calle Negocio, San Clemente, CA 92673 and further described as:

The BUSINESS PREMISES is a commercial office building located at 970 Calle Negocio, San Clemente, CA 92673. The sides of the building appear to be a stone facade, tan in color, with a pattern of large squares, approximately six feet in size cut into the facade. A white stripe appears at or near the top of the exterior walls of the building. The building number "970" appears in large numbers attached to the southeast side of the structure near the top above the white stripe. The "9" appears white in color and the "70" portion of the number appear black. Below and to the right of the building number is a business sign that reads "OC-IT.com" that includes a logo of three dots connected by two lines. Around the corner to the left of the building number, as viewed from the front of the building, the "OC-IT.com" sign and logo appear again. On both signs, the "OC" letters appear orange, the "IT" letters appear blue, and the "-" and the ".com" appear black. To the left the two "OC-IT.com" signs, as viewed from the front of the building, a third sign appears below the white stripe at the top of the wall that reads "Lightning Technology." The word "Lightning" in the sign

appears in green letters with the exception of the first "i" which appears as a large red lightning bolt. The word "Technology" appears below in black letters.

The public entrance to the BUSINESS PREMISES is located under the above-described signs on the southwest corner of the building. The door appears to be tinted glass in a white metal frame and the wall surrounding this door also appears to be tinted glass of the same shade with white metal trim arranged in a pattern of squares approximately three feet in size.

The BUSINESS PREMISES also has a pedestrian door on the rear of the structure on the northwest corner and a roll-up style warehouse door to the north of the pedestrian door.

The business entities "OC-IT.com" and "Lightning Technology" appear to share the same office space at 970 Calle Negocio, but the business space appears to be distinct from the attached space at 972 Calle Negocio which is described by a sign on the building at "San Clemente Gymnastics."

The BUSINESS PREMISES includes any attached or unattached structures, warehouses, garages, attics, basements, and assigned trash receptacles.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 17, United Stated Code, Section 506 - Criminal Infringement, Title 18, United States Code, Section 371 - Conspiracy, Section 1341 - Mail Fraud, Section 1343 - Wire Fraud, Section 2318 - Trafficking in Counterfeit Labels, Section 2319 - Criminal Infringement of a Copyright, and Section 2320 - Trafficking in Counterfeit Goods from March 2008 to the present, specifically:

a. Counterfeit Cisco transceivers, routers, switches, and computer networking equipment, and any accompanying accessories, labels, marks, letters of authenticity, and packaging.

b. Any document referencing or referring to counterfeit Cisco products or labels.

c. Any items bearing registered trademarks of Cisco.

d. Records, documents, programs, applications, and materials reflecting or referencing the importation, exportation, purchase, possession, transfer, distribution, or sale of Cisco transceivers, routers, switches, computer networking equipment, labels, and/or packaging.

e. Records, documents, programs, applications, and materials filed with U.S. Customs and Border Protection in

connection with the importation, exportation, purchase, possession, transfer, distribution, or sale of Cisco transceivers, routers, switches, computer networking equipment, labels, and/or packaging.

f. Business bank account records, wire transfer records, bank statements and records, money drafts, letters of credit, and financial transfers that reflect the money generated from the importation, exportation, purchase, possession, transfer, distribution, or sale of Cisco transceivers, routers, switches, and computer networking equipment.

g. Limited to 15 items per SUBJECT PREMISES, any records, documents, programs, applications, and materials that show indicia of occupancy, residency, control and/or ownership of the SUBJECT PREMISES, including but not limited to, utility bills, telephone bills, loan payment receipts, rent documents, canceled envelopes and keys, photographs, and bank records.

h. Records, documents, programs, applications, and materials reflecting off-site storage facilities owned, used, or operated by LIGHTNING TECHNOLOGY INC., OC-IT.COM, or MICHAEL WESTCOTT.

i. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

j. With respect to any digital device used to facilitate the above-listed violations or containing evidence

falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical

disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of

items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.